

## **REMARKS**

### **INTRODUCTION**

In accordance with the foregoing, no claims have been amended. Claims 1-55 are pending and under consideration.

### **CLAIM REJECTIONS**

Claims 1-55 were rejected under 35 USC 102(b) as being anticipated by Sugimura et al. (US 2003/0115473) (hereinafter "Sugimura").

Sugimura discusses a biometrics authentication system and method. In Sugimura, the biometrics authentication method includes conducting authentication of a user by a method other than biometrics authentication; registering and storing biometrics data regarding a user; determining whether or not biometrics authentication can be conducted by referring to stored biometrics data; conducting biometrics authentication; and outputting an authentication result as to whether the user is authenticated, wherein biometrics data on the user is registered and stored only in the case where the user is authenticated by the method other than the biometrics authentication, and biometrics authentication is conducted only in the case where it is determined that biometrics authentication can be conducted. Sugimura, Abstract.

#### **Claims 1-22, 45 and 46**

Independent claims 1 and 7 recite: "...determining whether the graphical password has been input..." In contrast to claims 1 and 7, Sugimura does not discuss a graphical password. A graphical password, as discussed by reference in the background section of the present application, is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words. The disclosure of Sugimura is directed to a biometrics authentication system. Although the background section of Sugimura mentions other authentication methods such as an ATM password using numbers and a digital certificate, nowhere does Sugimura discuss a graphical password. As such, it is respectfully submitted that claims 1 and 7 patentably distinguish over Sugimura.

Claims 2-6 and 8-22 depend on claims 1 and 7, respectively, and are therefore believed to be allowable for the foregoing reason. Further claims 45 and 46, reciting a computer readable medium to enable the methods of claims 1 and 7, are also believed to be allowable for the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

**Claims 23-44**

Independent claims 23 and 29 recite: "...a graphical password input unit which determines whether the graphical password has been input..." It is respectfully submitted that Sugimura does not discuss a graphical password input unit and therefore does not anticipate claims 23 and 29.

Claims 24-28 and 30-44 depend on claims 23 and 29, respectively, and are therefore believed to be allowable for the foregoing reason.

Withdrawal of the foregoing rejection is requested.

**Claims 47-51**

Independent claim 47 recites: "...comparing an input graphical password to a registered graphical password and outputting a valid result when the input graphical password is within a predetermined proximity window of the registered graphical password and outputting an invalid result when the input graphical password is outside the predetermined proximity window of the registered graphical password, wherein the user is authenticated when the valid result is output..." It is respectfully submitted that Sugimura does not discuss comparing an input graphical password to a registered graphical password, or graphical passwords at all, and therefore does not anticipate claim 47.

Claims 48-51 depends on claim 47, and are therefore believed to be allowable for the foregoing reason.

Withdrawal of the foregoing rejection is requested.

**Claims 52 and 53**

Independent claim 52 recites: "...authenticating a user by adjusting a biometric threshold based on comparing an input graphical password to an authorized graphical password, wherein the threshold is set to increase the possibility of the user being authenticated when the input graphical password matches the authorized graphical password and the threshold is set to decrease the possibility of the user being authenticated when the input graphical password does not match the authorized graphical password." It is respectfully submitted that Sugimura does not discuss comparing an input graphical password to an authorized graphical password, or graphical passwords at all, and therefore does not anticipate claim 52.

Claim 53 depends on claim 52, and is therefore believed to be allowable for the foregoing reason.

Withdrawal of the foregoing rejection is requested.

**Claims 54 and 55**

Independent claim 54 recites: "...a graphical password input unit which receives a graphical password input by a user, wherein a key manipulation unit is not used to input the graphical password..." It is respectfully submitted that Sugimura does not discuss a graphical password input unit, or graphical passwords at all, and therefore does not anticipate claim 54.

Claim 55 depends on claim 54, and is therefore believed to be allowable for the foregoing reason.

Withdrawal of the foregoing rejection is requested.

**CONCLUSION**

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Nov 13, 2006

By: Gregory W. Harper  
Gregory W. Harper  
Registration No. 55,248

1201 New York Avenue, NW, 7th Floor  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501